

## REMARKS

The Office Action dated November 20, 2009 has been carefully considered. In response to that Office Action, applicant requests amendment and reconsideration of the claims.

Claims 1-12, 14-15 and 17-22 are pending in the application. Claims 1 and 11 have been amended for the sake of clarity, to emphasize that the alarm event is an industrial control alarm event and that it occurs in a machine that is controlled by an "industrial controller", as already recited in the preamble.

The amendments to claims 1, 11 are appropriate under the standards established pursuant to 37 C.F.R. §1.116 and do not require any further search.

Claims 1 and 11 are rejected under 35 U.S.C. §112, second paragraph, as indefinite for allegedly lacking support for the "sensitive event-relevant information" recited in these claims.

Claims 1-4, 7-12, 14-15 and 17-22 stand rejected under 35 U.S.C. §102(e) as being anticipated by published U.S. Pat. Appl. No. 2008/0186166 of Zhou et al.

Claim 5 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Zhou et al. in view of Qi et al. (US 6892064).

Claim 6 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Zhou et al. in view of published U.S. Pat. Appln. No 2007/0208697 of Subramaniam et al.

### CLAIM REJECTIONS §112, SECOND PARAGRAPH

The rejection of claims 1-22 as indefinite under 35 U.S.C. 112, second paragraph is hereby respectfully traversed.

Applicant's invention is directed to solving the problem described in paragraphs [0003] to [0008] of the present application. Fewer technicians are used when industrial machines are highly automated and, as is well-known to one skilled in the art, these technicians are often not on site at all times -- they have become roving

technicians. These technicians who remotely supervise highly-automated industrial machines need to be highly mobile and to have immediate, secure access to detailed information from the controller of a machine that has caused an alarm condition.

As is well known, the more automated the industrial operation, the greater the potential losses from unauthorized access and improper acts. Thus, the more automated the industrial operation, the more event-relevant information that management regards as “sensitive”.

At the same time, the greater the degree of automation, the greater the amount of detailed event-relevant information that is needed by technicians and the greater the need for protecting the most sensitive parts of this event-relevant information from unauthorized access. [0006] In the case of the notorious Union Carbide industrial control alarm event in Bophal, India, skilled response to the sensitive information about impending process errors was a matter of life and death, and mistakes resulted in felony prosecutions.

Technicians have securely remotely accessed the event-relevant information provided by industrial controllers from a desktop computer, using PKI encryption, if they don't need to be roaming from place to place to inspect highly automated machinery. [0007] Similarly, whenever the technicians are on site, this information is securely directly accessed by on-site technicians from the machines' controllers, as illustrated by the numerical controller described in paragraph. [0003] However, since technicians are now often in the field inspecting and maintaining highly automated machinery, providing rapid remote access to information from the many industrial controllers that control the machines at the various locations served by a particular technician is a security problem. [0007] – [0008] That problem is advantageously solved by applicant's invention.

In sum, the “sensitive” information provided to technicians by industrial controllers in the claims is simply a subset of the information about an industrial control alarm event occurring in a machine it controls. That “sensitive” subset contains the information that can cause damage if used by unauthorized persons, as is well-known in industrial controller operations and discussed in paragraph [0006].

That information has been previously securely accessed either onsite, where the controller is protected from unauthorized access, or through PKI encryption, which also prevents unauthorized access.

The “sensitive” information within the “event-relevant” information that is written to a database in a machine’s controller is well-known in the art. PKI encryption protection is necessary for remote access to “event-relevant” information and, by definition, “event-relevant” information that needs encryption protection includes “sensitive” information. Thus, applicant’s recital of “sensitive” information that is included in the “event-relevant” information is not indefinite. Withdrawal of the rejection of claims 1 and 11 under 35 U.S.C. §112, second paragraph is thus respectfully requested.

#### **REJECTION UNDER 35 U.S.C. §102(e)**

The rejection of claims 1-4, 7-12, 14-15, and 17-20, as filed, under 35 U.S.C. 102(e) as anticipated by Zhou et al. is hereby respectfully traversed.

Zhou does not disclose writing event-relevant information about an alarm event occurring in a machine to the ASP database, and Zhou also does not write the event-relevant information to a machine’s industrial controller, as recited in applicant’s claims. Instead, Zhou writes the event-relevant information to a remote, multipurpose log and alarm service bureau (ASP) as seen in Fig. 1.

Furthermore, Zhou teaches away from writing the event-relevant information about an alarm event occurring in a machine to that machine’s industrial controller. Instead, Zhou teaches that centralizing diverse monitoring and alarm functions at a remote location -- instead of implementing them in the controller recited in applicant’s claims, which is necessarily on site -- is advantageous because many different types of customers can be served at the same, one, remote location. That one remote location is Zhou’s log and alarm service bureau, the ASP.

As described in paragraph [0003] of the specification, industrial machine controllers are located on-site with the machines they control, and provide direct

access to their event-relevant information to technicians who are on-site at the machine's location. These industrial controllers provide this direct access so that technicians can perform inspection and maintenance work on-site at the machine's location, as is well known in the art. Preferably, roving technicians responding to an alarm while at a remote location should be provided the same secure access to the information as the controller will provide to them when they are on-site with the machine looking at the controller.

Although Zhou does suggest providing tracking and monitoring of commercial food (Fig. 11) and hazardous waste (Fig. 13) shipments, landfill conditions (Fig. 13) at fixed locations and even controlling irrigation systems (Fig. 15), Zhou teaches that all should be done from the same remote location, not onsite! Even the irrigation control alarm is generated by that same remote, multipurpose ASP, not by an industrial irrigation controller. Zhou's irrigation valves are controlled by the ASP.

**[0215] – [0218]**

On the contrary, Zhou's remote service bureau (ASP) is advantageous because it centralizes all those different tasks and can generate alert messages based on sensed changes in location, as well as parameters monitored from fixed locations **[0005]**. Zhou's remote ASP is advantageous, and potentially profitable, because it can monitor so many different things, that is, because it is non-specialized and is at a fixed location that is remote from all of them.

In contrast, applicant's machines -- machine tools, robots, processing machines, etc. **[0003] - [0005]** -- are all already locally monitored and alarmed by their industrial controllers, as is well known in the art.

Specifically, applicant's alarm event-relevant information is written to that particular machine's controller, as recited in claims 1 and 11, rather than being written to the multipurpose service bureau disclosed by Zhou.

Industrial controllers are not general-purpose ASPs, such as Zhou's ASP. Because of the complexity of automated industrial equipment, each controller can only operate particular types of machines among the various machine tools, robots, processing machines, etc. described in paragraphs **[0003] - [0005]**. These particular

types of controllers for particular types of machines also cannot be remote from the machines they control. The industrial controllers must be located onsite with the machines they control, so as to permit inspection and maintenance of those machines. Also, for effective inspection and maintenance of the machines, the operational and alarm event-relevant information that their controllers provide, necessarily, the most up to date and complete information that can be obtained, apart from physically inspecting the machine's condition, as is well known in the art.

Thus, Zhou's remote, all-purpose ASPs cannot be the "industrial controller" recited in applicant's claims, by definition. This rejection is not supported by the cited art and should be withdrawn.

Furthermore, since applicant's invention is directed to securely communicating information that industrial controllers provide to technicians directly when the technicians are on site, the remote monitoring and alarm functions of Zhou's ASP are superfluous. Zhou is inapposite to applicant's invention.

Zhou neither discloses nor suggests the security problems of highly automated industrial machines and the problem of providing information that is local to an industrial control alarm event to the roving technicians who need it, nor applicant's solution of that problem. Withdrawal of the rejection of these claims under 35 U.S.C. §102(e) and allowance thereof are thus respectfully requested.

#### **REJECTION UNDER 35 U.S.C. §103(a)**

Rejection of Claim 5 as obvious over Zhou in view of Qi is hereby respectfully traversed.

Rejection of Claim 6 as obvious over Zhou in view of Subramaniam is also hereby respectfully traversed.

These claims depend indirectly and directly, respectively, from claim 1. Therefore they contain all the limitations thereof and those limitations patentably distinguish these claims over the applied prior art in the same manner as claim 1.

Withdrawal of the rejection of claims 5 and 6 under 35 U.S.C. §103(a) and allowance thereof are thus respectfully requested.

### CONCLUSION

In view of the above, each of the presently pending claims in this application is considered patentably differentiated over the prior art of record and believed to be in immediate conditions for allowance. Reconsideration and allowance of the present application are thus respectfully requested.

Should the Examiner consider necessary or desirable any formal changes anywhere in the specification, claims and/or drawing, then it is respectfully requested that such changes be made by Examiner's Amendment, if the Examiner feels this would facilitate passage of the case to issuance. If the Examiner feels that it might be helpful in advancing this case by calling the undersigned, applicant would greatly appreciate such a telephone interview.

Respectfully submitted,

By: 

Henry M. Feiereisen  
Agent For Applicant  
Reg. No: 31,084

Date: February 23, 2010  
708 Third Avenue  
Suite 1501  
New York, N.Y. 10017  
(212)244-5500  
HMF/RL:af